

RECEIVED  
CENTRAL FAX CENTER

AUG 03 2009

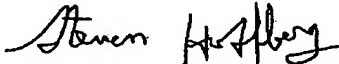
Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)

Approved for use through 04/30/2008. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional)	
		QMARK 201.2	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]  on _____  Signature _____  Typed or printed name _____	Application Number  10/791019	Filed  03-02-2004	
	First Named Inventor Eric Shepherd		
	Art Unit 2173	Examiner Shih, Haoshian	
Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.			
This request is being filed with a notice of appeal.			
The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.			
I am the			
<input type="checkbox"/> applicant/inventor.		/Steven M. Hoffberg/	
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)		Signature	
<input checked="" type="checkbox"/> attorney or agent of record. Registration number 33511		Steven M. Hoffberg	
		Typed or printed name	
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____		914-949-2300	
		Telephone number	
		August 3, 2009	
		Date	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input type="checkbox"/> *Total of _____ forms are submitted.			

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

QMARK 201.2

RECEIVED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE CENTRAL FAX CENTER

Applicant(s) : Shepherd, et al.  
Serial No. : 10/791,019  
Filed : March 2, 2004  
For : SECURE BROWSER  
Examiner : Haoshian Shih  
Art Unit : 2173

AUG 03 2009

August 3, 2009

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

PREAPPEAL CONFERENCE REQUEST

Claims 1-21 are rejected under 35 U.S.C. § 112, ¶1, as allegedly failing to comply with the written description requirement, for the recitation of "or a normal browser is to be employed" in claim 1, and "or whether an insecure browser is to be employed" in claim 9. It is initially noted that this language is part of the original claims, which itself provides sufficient "written description". Figs. 1 and 2 also clearly show the process for invocation of a secure browser, and the "data encoding type" or "data type encoding" as a basis for selecting the secure browser. See especially Fig. 2, "Participant runs browser (e.g. IE) normally", "Content includes triggering link to secure content" and "QSB delivers secure content". The specification includes an Appendix which includes operative code which implements various portions of the method, demonstrating authentication of the secure browser and launch of the secure browser (an error message if the launch fails). The specification makes clear that, if secure content (as determined based on its encoding) is not invoked, then a "normal browser" (insecure browser), e.g., Internet Explorer, is employed. It is noted that "normal" web browsers, such as Internet Explorer, open a new page from a selected hyperlink, typically in that same software. This behavior is fairly described in the specification, in addition to the modified behavior with respect to the secure content. The Written Description for a "normal browser", "secure browser" and an "insecure browser", and/or their equivalents, is found in at least the following passages: P. 1, l. 8-p. 3, l. 2; p. 5, l. 26-30; p. 10, l. 11-21, p. 11, l. 25-p. 12, l. 8; p. 13, l. 8-p. 14, l. 19; p. 15, l. 14-p. 17, l. 12. See Page 21, line 1-page 22, line 8, especially page 22, lines 1-8:

Using a PIP file like this, it means that users of corporate LMSs from companies like Saba, Plateau, Docent, Thinq, or academic course management systems like Blackboard and

QMark-201.2

- 1 -

WebCT, can invoke a secure browser without making any change to the LMS. Providing they can call Perception via one of the supported protocols via PIP, then a secure browser can come up when the assessment is taken – **the participant uses an ordinary browser to run the LMS and then a secure browser to take the assessment.**

It is therefore respectfully submitted that the application has ample support for the claim language, including a proper written description, to the extent that any such independent requirement exists under 35 U.S.C. § 112. Further, it is also clear that the claims are supported by an enabling specification and disclosure. Finally, the claims are definite, and lack ambiguity as to the scope of protection sought or its interpretation. The scope of the claims is also reasonably curtailed with respect to the scope of the disclosure.

Claims 1-4 and 6-20 are rejected as being anticipated under 35 U.S.C. § 102(e) over Winneg et al., US 7,069,586. Claims 5 and 21 are rejected as being obvious under 35 U.S.C. § 103(a) over Winneg et al., US 7,069,586 as applied to claims 1 and 9, respectively, in view of Chang et al., US 2002/0097416.

Winneg et al. is respectfully distinguished in that the secure application is invoked based on an identification and login credentials of a user which have nothing whatsoever to do with any “received data encoding type” (claim 1) or “received data type encoding” (claim 9), and the secure application is used to retrieve the protected content regardless of any such data encoding type or data type encoding. Applicant respectfully submits that a “user type” is clearly distinct and non-overlapping with an “data encoding type” or a “data type encoding”.

This difference can be clearly seen in Winneg et al. at Col. 25, line 52-Col 26, line 10:

...Before running the exam creation module, a user (e.g., a professor, instructor or teaching assistant) may create an exam content file by using a word processing application such as Microsoft Word. The exam creation module then may be used to provide a password for and/or encrypt the exam content file.

In a first act, the user may be prompted to enter the user's ID and password.

In a next act, the exam creation module may enable the user to locate the exam content file, for example, by enabling use of a browser application.

In a next act, the user may be prompted to enter a password that any students who will take the exam will be required to enter in order to take the exam and access the exam content file. The password and exam content then may be saved together in the exam content file.

As is be apparent, Winneg et al. defines the content and sources of information which are available only after login, and the determination of whether a secure “environment” or an

insecure/normal environment is not based on any “received data encoding type” or “received data type encoding”. Even if there are restrictions selective for particular exams, there is no teaching or suggestion that these restrictions are encoded in or as part of the document requested, but rather these are provided as set-up information for the secure application (Col. 17):

Accordingly, prior to performance of Act 146, any instances of the first application currently executing on the computer system may be terminated. To determine if an instance of the first application is currently executing on the computer system, a list of processes currently executing on the computer system may be accessed. The list may contain one or more entries, where each entry contains an identifier of a process currently executing on the computer system. Each entry may be accessed to determine whether the identifier of the entry is an identifier for the first application. If a match is found, the instance of the first application may be terminated and the identification of the instance may be removed from the list of currently executing processes.

Winneg et al. thus disclose that a secure application (which may include a secure browser-type application) is invoked, having predetermined restrictions, and only thereafter is a request for content issued from within the secure application, which does not change in dependence on the content itself or a respective content encoding. Different users can have different usage restrictions with respect to the same content—some users are test creators, some are test graders, some are test takers. Since the same content is treated differently, it clearly cannot be the *content* which controls the restrictions, and therefore the claims are distinguished. These restrictions are therefore based on the user login and the content *to be retrieved*, and such restrictions precede the content retrieval, are not established after the content is retrieved based on its encoding.

Likewise, since the secure environment is initiated before the request is made, and the secure environment does not normally terminate during use, insecure content cannot be employed within an insecure or normal browser. Thus, it is not disputed that Winneg et al. disclose a secure application. However, the disclosure of Winneg et al. is specific for an application which modifies the operating system environment, and Winneg et al. is not enabling in its description of how an invokable browser within that environment could perform the stated functions. Indeed, col. 16 precludes use of a normal browser, since this would permit the user to request uncontrolled content. This limitation arises because the secure application of Winneg et al. does not analyze a content type or content encoding:

Further, the first application may be configured such that hyperlink functionality is not available within the first application. Thus, a user cannot type in a uniform resource

locator (URL) and automatically launch a browser application that hyperlinks the user outside of the first application.

Likewise, Col. 19 states:

If Act 306 includes both looping through an authorized process list and looping through an unauthorized process list, the unauthorized process list may function as an added security measure. The unauthorized process list may include one or more processes that a controlling entity is particularly concerned about executing during execution of the first application. For example, the unauthorized process list may include browser applications, (e.g., Microsoft Internet Explorer), applications for scheduling tasks to be performed on the computer system, (e.g., Microsoft Task Scheduler), and applications for managing tasks performed on the computer system, (e.g., Microsoft Task Manager). Terminating task-managing manager and task-scheduling applications prevents a process (e.g., an application) that has been scheduled to execute during execution of the first application from executing.

Therefore, Winneg et al. employs a materially different method. For example, with respect of claim 1, the application of Winneg et al. which requests a document does not perform the step of "automatically determining, based on a received data encoding type, whether a secure browser or a normal browser is to be employed, the secure browser having a set of functionality restricted with respect to the normal browser, to enhance security of a received document against data export". Likewise, Winneg et al. does not perform the step of "automatically determining, based on a received data type encoding, whether a secure browser is required to be employed by a content provider or whether an insecure browser is to be employed, the secure browser restricting interaction of the user with tasks other than those permitted by the secure browser which are permitted by the insecure browser". The decision to use a secure application is made based on a user login, and independent of the "data encoding type" or "data type encoding".

Winneg et al. is thus respectfully distinguished in that a "professor" and a "student" can access the very same document (having the same data type encoding or data encoding type) and be afforded different privileges based on their login; in accordance with the presently claimed invention, it is the data which determines the browser as being "normal" or "insecure" on one hand, or "secure" on the other, not the user identification, which in turn defines the set of privileges available through the selected browser.

In formulating the rejection, the Examiner cites various portions of Winneg et al., which it is respectfully submitted do not teach or suggest at least the foregoing claim elements. For

example, the Examiner cites Col. 4, lines 3-5. However, at this passage, Winneg et al. state: "The application being securely executed may be of any of a variety of types of applications, for example, a browser application or an application for receiving answers to questions of an examination (i.e., an exam taking application)." Thus, while Winneg et al. appear to disclose a secure application, it fails to disclose that a normal or insecure browser is also selectively available, in dependence on a data type encoding or data encoding type.

The secure mode of Winneg appears to be initiated based on a boot sequence, operating system limitation or user login. Col. 6, lines 35-67. Col. 9, lines 45-47, 50-55 and Col. 10, lines 10-13 indicate that a user input (and not a data type encoding or data encoding type) determines which application to initiate. ("For example, FIG. 7 illustrates a GUI that may be displayed to a user to determine which application to initiate for the exam." "After the user has entered the class name and the professor in their respective fields and clicked on the OK button, the exam-taking application may use this information to determine a first application to be executed so that the student may take the exam (i.e., provide responses to one or more questions) and to determine the content (e.g., the questions of the exam or material to assist the user in taking the exam), if any, to be displayed by the first application." "Else, after hitting the 'OK' button of the GUI, next, in Act 122, secure execution of the exam-taking application may be initiated.").

Winneg et al. provides a system in which a local software application controls the client computer independent of a data type encoding or data encoding type. For example, Col. 6, lines 35-48 describe a system which defaults to a "secure" mode, and is machine status dependent, not received data encoding type or data type encoding dependent. Indeed, the authorization to access or delete an exam is provided within the "secure" mode, and thus these functions are all provided within a single secure application. Therefore, the decisions 114, 116 do not serve to switch different "browsers" which are normal/insecure and secure. Col. 8, lines 48- Col. 9, line 44. Throughout the entire exam process, the machine is locked in a "secure" mode, maintaining this mode apparently independent of data and its associated type encoding or encoding type.

Respectfully submitted,  
HOFFBERG & ASSOCIATES  
/Steven M. Hoffberg/  
Reg. No. 33,511

10 Bank Street-Suite 460, White Plains, NY 10606  
(914) 949-3100